PAUL HASTINGS

STAY CURRENT

May 2019

Follow @Paul_Hastings

Sanctions Compliance Shortfalls Result in $1 billion Global Enforcement Action

By Scott M. Flicker, Kwame J. Manley, Tom Best & Talya R. Hutchison

On 9 April 2019, the Financial Conduct Authority ("FCA"), the US. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the U.S. Department of Justice ("DOJ"), the New York Department of Financial Services ("NYDFS"), the New York County District Attorney's Office and the Board of Governors of the Federal Reserve System, announced action and settlements with Standard Chartered Bank ("SCB") resulting in an aggregate of over US$1 billion in fines. Broadly, these matters related to money laundering and financial sanctions failings.

In the UK, the FCA's enforcement action focused on what the bank identified as higher risk business lines, being its correspondent banking business and its branches in the United Arab Emirates ("UAE"). The action taken in the United States focused on potential liability arising from transactions that were processed to or through the United States in violation of Iran, Cuba, Sudan, Syria, and Burma sanctions.

This global enforcement action and major settlement targeting alleged breaches of U.S. sanctions by a non-US financial institution is the latest example of the increasing cooperation among enforcement authorities in and outside the United States focusing on alleged financial crime failings by banks. The various orders demonstrate a regulatory emphasis on SCB's apparent lack of adequate compliance structures to manage the risk of violation of these complex multi-jurisdiction requirements. In addition to fines and revisions to policies and procedures, the various settlements in the United States contain provisions whereby regulators preclude individuals involved in the improper conduct from any direct or indirect future involvement at SCB. This coincides with the DOJ's announcement that one of SCB's former employees involved in the alleged misconduct pled guilty in the District of Columbia for conspiring to defraud the United States and to violate the International Emergency Economic Powers Act ("IEEPA").

The FCA's Action

The FCA's action against SCB has been taken under the Money Laundering Regulations 2007 (the "Regulations"). These have of course been replaced in the UK by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. However, the FCA's Relevant Period ended in December 2014, when the 2007 Regulations were still in force.

When taking action against firms for anti-money laundering ("AML") contraventions, the FCA has a choice as to whether to take action for contravention of regulatory systems and controls requirements (e.g., under the Principles for Businesses or SYSC requirements) or whether to take action under the Regulations, which opens the door to the imposition of a civil fine or a criminal prosecution. In a speech given on 4 April 2019 Mark Steward, the FCA's Director of Enforcement, stated that the FCA is now conducting "*dual track*" AML investigations, that is investigations into breaches of the Money Laundering Regulations which might give rise to either civil or criminal

proceedings. The case against SCB was brought under the civil track and resulted in the imposition of a fine of £102 million.

In broad terms, the FCA's action highlights the need for firms operating internationally to ensure that UK standards are applied equally in all jurisdictions in which the firm operates. In fact, the need to for proper policies, procedures and controls might be even greater outside the UK, given higher risks of money laundering and terrorist financing that might be associated with some jurisdictions. Certain aspects of the FCA's action against the bank relate to business associated with Iran, a country which is subject to financial sanctions programmes. This also featured in the action taken in the US. The FCA's action also highlighted the need for firms to properly resource their control functions both in terms of quantity and quality of staff.

More specifically, in its Final Notice the FCA found the following failings in relation to the banks UAE Branches.

- SCB failed to ensure the AML controls which it required its UAE branches to apply were at least equivalent to those required of a UK firm.

- Specific failings in this respect related to a failure to collect sufficient information on the customer and the analysis of information obtained in order to understand the nature and purpose of the customer's accounts and businesses. The FCA also found that the firm had consistently failed to establish the source of funds of the customer to enable an assessment of whether the risks associated with the customer were likely to materialise.

- An example provided by the FCA of this failing included the firm accepting a cash deposit of around £500,000 on the opening of an account in circumstances where the customer file contained little evidence that the source of these funds had bene investigated or whether potential financial crime risks had been considered at the account opening.

- In relation to its correspondent banking relationships, the FCA found that SCB should have carried out an assessment of the quality of the AML controls of its respondent banks, including establishing whether these controls met internationally recognised standards. Whilst SCB incorporated the assessment of the quality of a respondent's supervision in their country risk rating, the FCA's file review found that in 88% of cases, there was insufficient evidence that the firm had assessed adequately the quality of the respondent's AML controls.

- Ongoing monitoring has featured consistently in enforcement action that the FCA has taken. In relation to SCB the FCA found that there had been widespread failures in the firm's reviews of due diligence conducted as part of its ongoing monitoring of AML risks from customer accounts.

- The FCA also identified certain governance failings which it described as deficiencies in the oversight of AML risks and controls. Checks carried out as part of the first and second lines of defence were found not to be effective and did not provide an appropriate level of scrutiny and challenge. The firm's Financial Crime Risk function was, according to the FCA, under-resourced in terms of quantity and quality. The FCA stated that staff were overworked and overloaded.

- The FCA further found that the firm had not appropriately identified and mitigated AML risks in its UAE branches and that the firm had not approached these matters in a holistic or proactive manner. One issue was that the firm's services could be accessed through various channel which could permit customers from higher risk jurisdictions to access SCB's services. For example, customers in Iran and other sanctioned countries could

> access the bank's online banking system for retail customers. While this risk was identified, the bank did not block access from relevant jurisdictions for a material period of time after the identification of the issues.

The FCA's Final Notice recognises positively that SCB has taken various significant remedial steps in relation to these matters.

Action in the United States

From June 2009 until June 2014, SCB processed to or through the United States 9,335 United States Dollar ("USD") denominated transactions that involved persons or countries subject to comprehensive sanctions programmes administered by OFAC. These transactions totalled over US$430,000,000.

The U.S. agencies focused their investigations on transactions involving Iran-related accounts maintained by SCB's Dubai, UAE branches ("SCB Dubai"), including accounts at SCB Dubai held for a number of general trading companies and a petrochemical company. SCB Dubai processed USD-denominated transactions to or through SCB's branch office in New York or other U.S. financial institutions on behalf of customers that sent payment instructions to SCB Dubai; these customers were physically located in and/or were residents of Iran.

The investigations revealed that a majority of the USD-denominated transactions were transmitted to SCB Dubai through SCB's fax and online payments system at the Dubai branch. In order to avoid detection by U.S. financial institutions or regulators, employees of SCB Dubai developed "*ways to structure financial transactions that would not raise suspicion of an Iran connection*" and that involved providing "*false and misleading information in order to disguise the Iranian connections.*"

In reaching the settlements, regulators focused on SCB's lack of global compliance controls and failure to address red flags that would have prevented transactions with countries embargoed under U.S. law. OFAC's press release explained that "*SCB's compliance program was inadequate to manage the bank's risk and suffered from multiple systemic deficiencies, including failure to respond to warning signs in a timely and efficient manner.*" OFAC found that despite "*multiple supervisory employees and management personnel*" being aware of potential access to SCB's online systems in Iran, the Bank failed to adequately implement controls to block access. This is similar to issues that the FCA also identified.

Prosecutors also announced the guilty plea of an anonymous employee of the Bank's Dubai branch involved in the misconduct. Referred to as Person A in the amended Deferred Prosecution Agreement, the employee pled guilty to conspiring to defraud the United States and to violate the IEEPA. Commenting on prosecuting individuals involved in sanctions violations, U.S. Attorney Jessie K. Liu of the District of Columbia stated:

> "*When bank employees and customers conspire to violate U.S. sanctions and subvert our national security, we will bring them to justice no matter where they reside or operate.*"

SCB also agreed with the Federal Reserve and NYDFS to hold accountable individuals involved with the alleged conduct by prohibiting them from any future involvement with the Bank. Specifically, SCB agreed not to retain any individual as an officer, employee, agent, consultant, or contractor who was found to have "*participated in the illegal conduct . . .* [and] *been subject to formal disciplinary action as a result of Standard Chartered's internal employee accountability review*" and who "*has either separated from Standard Chartered or has had his or her employment terminated.*"

Collectively, SCB agreed to settle multiple alleged violations of the IEEPA, including two felony counts of conspiracy to violate the IEEPA, New York banking laws, and various AML regulations. The settlement required that SCB extend its prior Deferred Prosecution Agreement with the DOJ for an additional two years.

Compliance Considerations

As part of the settlement, SCB agreed to adhere to ongoing compliance commitments related to Management, Risk Assessment, Internal Controls, Testing and Audit, Training, and Annual Certification. These compliance commitments are consistent with the "*five pillars*" of an effective AML and Bank Secrecy Act compliance program, as established by the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

The SCB settlement highlights U.S. and U.K. regulators' continued focus on compliance, and their specific attention to the lapses in internal controls which led to the alleged violations.

Key Takeaways

- The global coordinated effort by state, federal, and non-US enforcement agencies suggests that companies should be prepared to manage simultaneous complex internal investigations addressing complex legal and regulatory requirements in various jurisdictions.

- Based on the requirements set forth in the OFAC settlement, both financial and non-financial institutions should examine their compliance programs against FinCEN's "*five pillars*" of an effective compliance program.

- Where a company has significant lapses in internal controls and ignores red flags, the settlements suggest that regulatory agencies are more likely to conclude that the violations were egregious and/or criminal, significantly increasing the company's exposure.

- Individuals may also face criminal prosecution, no matter where those individuals are located. As part of any internal remedial efforts, companies should take a proactive approach to consider whether individuals should be barred from any future employment with the company. Moreover, employees should be aware that a company-centric settlement could effectively result in a bar on future employment without the due process of a specific enforcement action being brought against the employee.

- All companies should instruct senior management to take immediate action to address any red flags suggesting potential involvement with sanctioned jurisdictions.

Something Familiar, Something New: OFAC's Compliance Programme Framework

The recent actions involving Standard Chartered Bank have once again emphasised the risk of contravening U.S. financial sanctions requirements. A number of non-U.S. firms have been subject to significant penalties in this respect. Given this, recent guidance issue in the U.S. in connection with expectations around sanctions compliance programmes will assist firms in mitigating risks.

The U.S. Department of the Treasury's Office of Foreign Asset Controls ("OFAC") released its "*A Framework for OFAC Compliance Commitments*" (the "Framework") on 2 May 2019.[1] The Framework outlines what OFAC views as the essential components of a Sanctions Compliance Programs ("SCP"). In order to comply effectively with economic sanctions restrictions and requirements, many companies choose to implement risk-based SCPs. This guidance, however,

marks the first time that OFAC has provided explicit guidance to companies on its views of what should be included in an effective SCP, and appears to signal the latest instalment in its subtle-but-steady push to communicate more with the economic sanctions user community regarding its enforcement and compliance expectations.

Many of the concepts will be familiar to compliance professionals generally, as sensible baseline compliance measures that any program addressing cross-border risks would naturally include. Some suggested measures, however, are tailored to specific risks that arise in the sanctions compliance context; other measures one might expect to see addressed are not included.

The OFAC guidance comes at a time when economic sanctions have come to occupy a position of greater prominence in the regulation of cross-border economic activity and as U.S. officials continue to ramp up both the number of enforcement actions and the range of penalties imposed. Recent prominent settlements have included a requirement that the targeted company implement compliance measures that closely mirror the elements of the SCP. OFAC is clearly seeking to leverage the impact of its enforcement activity to encourage companies globally to adopt preventative measures. OFAC may also be seeking to close the "guidance gap" between it and the other U.S. agencies concerned with cross-border legal risks, including the Department of Justice ("DOJ"), whose National Security and Criminal divisions have issued extensive compliance and enforcement guidance in recent years.[2] Ever-present requests for guidance from the private sector may also have been a catalyst.

Now that OFAC has provided this communication, OFAC will likely come to expect more from companies that previously may have pleaded ignorance as to what would be sufficient for a risk-based SCP for an organization. In issuing this Framework, OFAC expressly stated that it would now consider "the existence of an effective SCP" in determining penalty calculations for violations.[3]

The Framework

The Framework sets out OFAC's position that an effective SCP contains the "five essential components of compliance":

1. management commitment;
2. risk assessment;
3. internal controls;
4. testing and auditing; and
5. training.

The Framework explains in some detail what OFAC views as the elements of each component.[4] OFAC also includes an appendix outlining ten "root causes" of past sanctions violations, explaining how they have led to enforcement actions in certain types of enterprises since the publication of OFAC's Economic Sanctions Enforcement Guidelines.[5]

The Five Components

OFAC has long included a Risk Matrix in its Economic Sanctions Enforcement Guidelines ("Guidelines") as an appendix to the OFAC federal regulations as a way for financial institutions to "*evaluate their compliance programs.*"[6] Several elements of the matrix are now included in the more detailed and precise Framework. While OFAC acknowledges that the level of complexity and sophistication required for an SCP will vary depending on company-specific factors, the five

components on which an SCP should be predicated remain the same, which are identified and explained as follows.

Management Commitment

OFAC considers senior management's commitment to a company's SCP as "*one of the most important factors in determining its success,*" and has set out five ways that a company's senior management—including its senior leadership and the board of directors—should be involved in an effective SCP :[7]

1. Reviewing and approving the company's SCP;

2. Ensuring the compliance function has the requisite authority and autonomy to be effective, including direct reporting lines to senior management;

3. Providing the compliance function with adequate resources, such as personnel and technology;

4. Promoting a "culture of compliance" throughout the company; and

5. Demonstrating recognition of the severity of OFAC violations and implementing appropriate measures to ensure compliance with sanctions.

OFAC emphasizes that in order for an SCP to be adequately resourced, a company should maintain a "dedicated OFAC sanctions compliance officer," who—in a nod to the many hats most compliance officers often wear—may be someone serving in other senior compliance positions. Demonstrating that a company has a single individual who is responsible for sanctions compliance oversight is a simple, but significant, way to exhibit a management commitment to sanctions compliance.

Risk Assessment

As with similar documents published by the DOJ, SEC, and other enforcement agencies concerned with foreign corruption and other wrongdoing, the Framework explicitly states the need for companies to conduct tailored risk assessments.[8] Unlike those documents, however, the Framework does so in a more focused and targeted way, emphasizing three key areas that companies may assess in order to determine areas where a company may engage with sanctioned persons or jurisdictions:

1. Third parties (i.e., customers, supply chain, intermediaries, and counter-parties);

2. Product and service offerings; and

3. Geographic locations of the company.

OFAC encourages companies to conduct a risk assessment both "*in a manner, and with a frequency, that accounts for the potential risks.*" Accordingly, OFAC provides that a "central tenet" of an effective risk assessment is ensuring that it is routine and, if appropriate, ongoing. Risk assessments can most effectively assist in creating internal controls and training when companies update and adapt the assessment periodically, in order to account for any underlying root causes that have led to deficiencies within the organization that could lead to sanctions violations.

Internal Controls

The Framework explicitly sets out seven key internal controls that should be included in an SCP.[9] Implementing these controls provide an organization with the policies and procedures necessary to

minimize risk and identify, escalate, remedy, and keep reports of potential sanctions violations. The seven internal controls that OFAC explains are:

1. Written policies and procedures that are easy to follow and designed to prevent employees from engaging in misconduct;

2. Internal controls such as technology solutions that are calibrated to appropriately address the company's risk profile;

3. Internal or external audits designed to enforce the policies and procedures;

4. Recordkeeping policies to adequately account for any requirements imposed by sanctions programs;

5. Mechanisms to take immediate and effective action to remedy internal controls when a weakness is identified;

6. Clear communication of the SCP policies and procedures to relevant personnel and third parties; and

7. Appointment of personnel to integrate the SCP into the daily operations of the company.

Interestingly, OFAC emphasizes that in order to be effective, SCP "*should be capable of adjusting rapidly to changes published by OFAC*"—including changes to lists of blocked persons, new or updated sanctions, and the issuance of general licenses.

Testing and Auditing

While many of the Framework components were previously considered in the Guidelines and are common across all compliance disciplines, testing and auditing was not previously included in such guidance and represents a new piece of the compliance puzzle. Companies are encouraged to conduct audits to discover discrepancies between the ideal practices as set forth in the SCP, and day-to-day operations of a company.[10] OFAC now expects to see at least three attributes in connection with the sanctions audit function, including a company's commitment to ensuring:

1. The audit function is accountable to senior management and equipped with the necessary tools and resources;

2. The audit procedures are appropriately scaled to the company's level of commercial sophistication; and

3. The company will take immediate action to remedy any issues identified by the audit.

Auditing is an important mechanism by which companies can analyze the effectiveness of the policies and procedures implemented by an SCP, and OFAC now expressly considers a company's commitment to such practices.

Training

As one would expect, OFAC identifies effective training as an "integral component of a successful SCP." OFAC further explains that, for a training program to be considered adequate by the agency, a company must:

1. Ensure the program is tailored effectively to provide appropriate levels of information to all relevant employees;

2. Confirm the scope of the program is proportional to the company's specific circumstances, such as third parties with which the company deals, its products and services, and its geographic presence;

3. Provide the training with suitable frequency based on the company's risk profile;

4. Institute training upon learning of a deficiency related to sanctions compliance; and

5. Include easily accessible resources as a part of the training program.

The Framework is very prescriptive in this section; OFAC provides that the training should not only be periodic, but at a minimum annually. In addition to providing these general aspects, OFAC also explains that the training should provide job-specific knowledge, communicate responsibilities to each employee, and hold employees accountable for knowledge of sanctions compliance through assessments. Training programs are now necessary under this Framework.

What is Not Found in the Five Components

For all the valuable granularity in the Framework, there are some common compliance programme items which appear in guidance documents in other areas and which one might have expected OFAC to include—but evidently, deliberately did not.[11] Those items include, among others, a confidential reporting process, an investigations process (as opposed to auditing of the SCP as in the Framework), disciplinary measures for employees which fail to follow the program, an emphasis on "message in the middle" (as opposed to "tone from the top"), and a number of other nuances.

It is not clear why OFAC chose to omit these nuances where many of the companies to which the Framework applies will also be subject to more general DOJ Criminal Division compliance guidance, but no doubt practitioners will seek further clarification from OFAC in the weeks and months to come.

The "Root Causes"

In what appears to be somewhat of an innovation in the cross-border compliance community, the Framework also includes an Appendix setting out ten different root causes OFAC states it often sees as the reasons for sanctions violations.[12] We find this portion of the Framework helpful and believe it will be for companies as well, as they assess their own programs in the context of those basic issues that have led to enforcement actions over the last ten years.

These root causes include:

1. Failure to maintain an SCP at all;

2. Misinterpreting the applicability of sanctions;

3. Non-U.S. persons facilitating transactions with sanctioned parties;

4. Exporting or re-exporting U.S.-origin goods, technology, or services to sanctioned persons or countries;

5. Utilizing the U.S. financial system for transactions with sanctioned persons, including by conducting the transaction in U.S. dollars;

6. Relying on faulty or outdated sanctions screening software;

7. Conducting improper due diligence on third parties;

8. Inconsistent application of a compliance programme;

9. Using non-standard commercial practices; and

10. The actions of individuals who cause companies to be liable for sanctions violations.

Companies may use these root causes as a tool to identify what kinds of issues may be particularly applicable to them given their specific set of facts and circumstances such as commercial sophistication and international presence. While each of these root causes could be discussed at length in their own right, two root causes warrant particular emphasis: (i) the failure to maintain any formal SCP; and (ii) individual actions that lead to liability.

The Importance of Having an Effective SCP

Though sanctions violations are often caused by a confluence of events, the first root cause of sanctions violations OFAC lists is the lack of a formal OFAC SCP. Without an effective SCP, companies can engage in the regular course of business with the best of intentions but ultimately be unable to identify threats of sanctions violations because of a lack of policies or procedures designed to catch such risks. Companies without such a programme therefore run the risk of unknowingly engaging in sanctioned business and forfeiting the opportunity to voluntarily disclose it to OFAC in a manner that would demonstrate a commitment of compliance with sanctions regulations.

OFAC indicates that in past enforcement actions, it has considered the lack of an SCP to be an aggravating factor that increases the civil monetary penalty. Now that OFAC has issued the Framework wherein it says it would consider "favourably" the existence of an SCP when a violation occurred, ineffective compliance policies that do not comport to OFAC's stated guidance also run the risk of becoming an aggravating factor.

Having an effective SCP is the gateway to sanctions compliance, and many of the additional root causes identified by OFAC as causing sanctions violations may be eliminated by having such a compliance program in place.

The Risk of Individual Liability

OFAC's inclusion of the "actions of individuals" as a root cause, and its explicit acknowledgement that it may seek to hold individuals and companies liable for sanctions violations, is a new development in OFAC's public messaging.

It may be intended to reemphasize the DOJ's 2016 guidance on voluntary self-disclosures, cooperation, and remediation in instances of sanctions and export control violations ("NSD Guidance"). The NSD Guidance, which paralleled similar guidance relating to the then-FCPA Pilot Program and incorporated the so-called Yates Memorandum, explained that in voluntarily disclosing violations to the DOJ, companies must disclose known relevant facts, including those pertaining to the specific individuals involved in the violations.

An effective SCP is not only important in protecting companies against aggressive OFAC enforcement, but also any such individual employees who may have played "integral roles in causing or facilitating" sanctions violations.

Bottom Line

While many of the five enumerated elements of the SCP are common elements of sophisticated compliance programmes, they are now all but mandatory in OFAC's opinion. In publishing not only specific elements of an SCP that OFAC deems "essential," but also detailing the ten root causes of violations, OFAC may be signaling an era of increased enforcement actions. In 2019, OFAC has

already issued 14 penalties or settlements.[13] In 2018, OFAC only issued seven in the entire year; in 2017, OFAC issued 16 in total.

This Framework and outline of root causes of sanctions violations provide a clear roadmap for OFAC to evaluate how ineffective compliance programs give rise to sanctions violations. In an environment with increasingly turbulent sanctions regime, assurance that a company's SCP is in line with OFAC expects it must become the norm. If a company's SCP does not meet these standards, the company may be at risk for penalties that are otherwise preventable.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

Randall V. Johnston
1.212.318.6664
randalljohnston@paulhastings.com

Timothy L. Dickinson
1.202.551.1858
timothydickinson@paulhastings.com

Kwame J. Manley
1.202.551.1962
kwamemanley@paulhastings.com

Washington, D.C.

Tom Best
1.202.551.1821
tombest@paulhastings.com

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

Charles A. Patrizia
1.202.551.1710
charlespatrizia@paulhastings.com

Talya Hutchison
1.202.551.1930
talyahutchison@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.comc

Robert D. Luskin
1.202.551.1966
robertluskin@paulhastings.com

---

[1] *A Framework for OFAC Compliance Commitments*, U.S. Department of the Treasury, Office of Foreign Assets Control (May 2, 2019), https://home.treasury.gov/news/press-releases/sm680 (hereinafter, the "Framework").

[2] *See Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations*, U.S. Department of Justice, National Security Division (Oct. 2, 2016), https://www.justice.gov/nsd/file/902491/download; The Evaluation of Corporate Compliance Programs, U.S. Department of Justice, Criminal Division (Apr. 30, 2019), https://www.justice.gov/criminal-fraud/page/file/937501/download.

[3] OFAC will now consider the existence of an effective SCP in its determination of whether or not a violation of sanctions regulations is considered to be "egregious." The Director or Deputy Director makes determinations of whether a violation is egregious for purposes of calculating monetary penalties. A determination that a violation was egregious leads to larger penalties, up to the statutory maximum if the case is egregious and the violation was not self-disclosed. The current statutory maximum penalty for violations of the International Emergency Economic Powers Act, under which many sanctions programs are promulgated, is the greater of $295,141 or twice the amount of the underlying transaction for each violation.

[4] Framework, *supra* note 1, at 1.

[5] *Id.* at 9.

[6] 31 C.F.R. Part 501, Appendix A.

[7] Framework, *supra* note 1 at 2.

[8] *Id.* at 3.

[9] *Id.* at 5.

[10] *Id.* at 6.

[11] *See generally The Evaluation of Corporate Compliance Programs*, *supra* note 2.

[12] Framework, *supra* note 1 at 9.

[13] See Civil Penalties and Enforcement Information, U.S. Department of the Treasury, https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx.